~~TOP SECRET//SI//NOFORN~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL

REPORT OF INVESTIGATION

17 July 2014

IV-13-0095

Failure to Submit a Timely Intelligence-Related Incident Report

(U) This report might not be releasable under the Freedom of Information Act or other statutes and regulations. Consult the NSA/CSS Inspector General Chief of Staff before releasing or posting all or part of this report.

~~TOP SECRET//SI//NOFORN~~

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the NSA Director and by statute, the Office of the Inspector General conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources by the Agency and its affiliates, and ensure that NSA activities comply with the law. The OIG also serves as an ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and their internal controls. Financial audits determine the accuracy of the Agency's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS

(U) The OIG administers a system for receiving complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations may be undertaken in response to those complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) INTELLIGENCE OVERSIGHT

(U) Intelligence oversight is designed to insure that Agency intelligence functions comply with federal law, executive orders, and DoD and NSA policies. The IO mission is grounded in Executive Order 12333, which establishes broad principles under which IC components must accomplish their missions.

(U) FIELD INSPECTIONS

(U) Inspections are organizational reviews that assess the effectiveness and efficiency of Agency components. The Field Inspections Division also partners with Inspectors General of the Service Cryptologic Elements and other IC entities to jointly inspect consolidated cryptologic facilities.

I. (U) SUMMARY

(b)(3)-P.L. 86-36
(b)(6)

(U//~~FOUO~~) This investigation was conducted in response to a complaint alleging that [redacted] failed to report a violation of the Foreign Intelligence Surveillance Act (FISA).

(U//~~FOUO~~) The complaint alleged that on 9 September 2013 FISA information which had exceeded the one year retention authority was discovered in a data repository within [redacted] and that [redacted] was told about the retention violation. The FISA information was deleted on 10 September 2014. Although [redacted] was told that FISA information was being retained longer than permitted on 9 September 2013, she did not report the unauthorized retention violation to the Signals Intelligence Directorate (SID) Oversight and Compliance office until after being interviewed by the OIG on 26 September 2013. (b)(3)-P.L. 86-36

(U//~~FOUO~~) United States Signals Intelligence Directive (USSID) SP0018, Legal Compliance and U.S. Persons Minimization Procedures, dated 25 January 2011 states that, for retention, "sufficient duration is one year unless the Deputy Director for Operations, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence activities." SID Oversight and Compliance FISA-Related Responsibilities Memorandum, dated 10 August 2006, requires that SID Oversight and Compliance be notified "immediately" of any FISA incidents that stem from improper collection, processing, retention, or dissemination. USSID SP0019, NSA/CSS SID Oversight and Compliance Policy, dated 13 November 2012, requires that a collection incident "must be reported" to local management and Oversight and Compliance "upon recognition, or as soon as practicable."

(U//~~FOUO~~) Based upon the preponderance of the evidence, the OIG concludes that [redacted] failed to notify SID Oversight and Compliance of a FISA incident upon recognition, or as soon as practicable. [redacted] failure to report this FISA incident in a timely manner was in violation of SID Oversight and Compliance FISA-Related Responsibilities Memorandum and of USSID SP0019, NSA/CSS SID Oversight and Compliance Policy.

(U//~~FOUO~~) A copy of this OIG report will be forwarded to MR, Employee Relations, for information and appropriate action.

II. (U) BACKGROUND

(b)(3)-P.L. 86-36

(U) Introduction

(U//~~FOUO~~) [redacted] branch maintains data repositories that have strict age-off scripts[1] to ensure that all [redacted] FISA information is removed from databases and file systems after being retained for one year. On 9 September 2013 [redacted] discovered that FISA information that exceeded the one year retention authority was being stored in the [redacted] directory. This [redacted] directory is not accessible to analyst query. Data is stored there to comply with Agency continuity of operations planning.

(U//~~FOUO~~) The age-off scripts were written to capture and delete FISA information older than one year [redacted] The FISA information which eluded the age-off scripts entered into the [redacted] There were approximately [redacted] zip files identified that contained FISA information that had been retained beyond the one year authority. The FISA information exceeded the one year retention authority between one and approximately one hundred days.

(U//~~FOUO~~) Software developers assigned to the [redacted] branch have since deleted all FISA information that was being retained beyond the one year authority and have written new age-off scripts to capture FISA data received [redacted]

(U//~~FOUO~~) The [redacted] branch submitted detailed reports of the FISA information retention violation to the SID Oversight and Compliance office and the NSA Office of General Counsel after being contacted by the OIG on 26 September 2013.

(U) Applicable Authorities

(U) The following authorities are applicable to this investigation. The details of the following authorities are included in Appendix A.

- (U) United States Signals Intelligence Directive USSID SP0018 Legal Compliance and U.S. Persons Minimization Procedures
- (U) United States Signals Intelligence Directive USSID SP0019 NSA/CSS Signals Intelligence Directorate – Oversight and Compliance Policy
- (U//~~FOUO~~) Signals Intelligence Directorate Oversight and Compliance Information Memorandum, FISA-Related Responsibilities

[1] (U) An age-off script is a software program that is designed to automatically delete information after that information reaches a certain age.

III. (U) FINDINGS

(U//~~FOUO~~) Issue: Did [redacted] fail to report the improper retention of FISA data upon recognition, or as soon as practicable?

(U//~~FOUO~~) **CONCLUSION: Substantiated.** *The preponderance of the evidence supports the conclusion that [redacted] failed to report the improper retention of FISA data, a FISA incident, upon recognition, or as soon as practicable, in violation of USSID SP0019, NSA/CSS Oversight and Compliance Policy and SID Oversight and Compliance Memorandum, FISA-Related Responsibilities.*

(U) Documentary Evidence

(b)(3)-P.L. 86-36
(b)(6)

(U//~~FOUO~~) **NSA/CSS Intelligence-Related Incident Report.** On 26 September 2013 a NSA/CSS Intelligence-Related Incident Report was submitted by [redacted] Deputy Chief, [redacted] concerning the improper retention of FISA information that was discovered on 9 September 2013 (Appendix B).

(U//~~FOUO~~) **Email from [redacted] to [redacted] management, 26 September 2013.** This email from [redacted] to her management chain describes the discovery of the FISA information retention violation on 9 September 2013. This email informed [redacted] management that a FISA incident report was not submitted when the FISA information retention violation was discovered but that an incident report would be forthcoming(Appendix C).

(U//~~FOUO~~) **Email from [redacted] to [redacted] management, 10 September 2013.** This email from [redacted] to her management chain informs them that the FISA information that was being retained beyond the retention authority had been deleted (Appendix D).

(U) Testimonial Evidence

(b)(3)-P.L. 86-36

(U//~~FOUO~~) [redacted]

(U//~~FOUO~~) [redacted] was interviewed on 26 September 2013. [redacted] provided the following sworn testimony.

(U//~~FOUO~~) [redacted] has been assigned to the [redacted] branch since January 2007. She has been the chief of this branch since November 2012.

(U//~~FOUO~~) [redacted] said that the [redacted] branch develops and maintains data bases in support of [redacted] The information that the [redacted] branch receives from [redacted] contains FISA information. The [redacted] branch is allowed to retain FISA information for a period not to exceed one year. The [redacted] software analysts have designed programs to automatically age off (delete) FISA information after one year.

(U//~~FOUO~~) On 9 September 2013 a contractor assigned to the [redacted] branch notified [redacted] that FISA information was being retained beyond one year. The next day [redacted] reported this retention violation by email to her immediate managers. [redacted] said that she did not make any further notifications to Agency officials. [redacted] said that she was waiting for a report on the extent of the FISA retention violation from the analyst who wrote the automatic age off scripts but that she forgot to ask the analyst for that report.

(U//~~FOUO~~) [redacted] said that she knows she should have submitted an Intelligence-Related Incident Report to the Oversight and Compliance office to report the unauthorized retention of FISA information once she was notified of the retention violation. [redacted] said that she knows the "onus" is on her to report the unauthorized retention of FISA information but that she "got busy" with other work.

(U//~~FOUO~~) [redacted]

(U//~~FOUO~~) [redacted] was interviewed on 26 September 2013 and 15 January 2014 and provided the following sworn testimony.

(U//~~FOUO~~) [redacted] has been assigned to the [redacted] branch since 2004 and has been the deputy chief of that branch since January 2013.

(U//~~FOUO~~) [redacted] said that the retention of FISA information has a very strict one year retention authority. Agency policy requires that incidents involving the retention of FISA information beyond one year constitutes a violation of FISA handling authorities which must be reported to the SID Oversight and Compliance office within 24 hours of discovery.

(U//~~FOUO~~) [redacted] said that on 9 September 2013 a contractor working in the [redacted] branch discovered that FISA information was being retained longer than one year. On 10 September 2013 this unauthorized retention was confirmed by the software developer who had written the program to automatically age off FISA information once it had reached its one year retention date. The FISA information that had been retained longer than one year was deleted. [redacted] said that she and [redacted] were notified of the retention violation on 9 September 2013.

(U//~~FOUO~~) [redacted] said that [redacted] sent an email to their management chain to notify them about the FISA information retention violation. However, [redacted] did not report this retention violation to SID Oversight and Compliance via an Intelligence-Related Incident Report as required: "I can honestly tell you that I don't believe anybody turned in that incident report that should have been turned in."

(U//~~FOUO~~) [redacted] said that it was "definitely" the fault of management for not submitting an Intelligence-Related Incident Report to SID Oversight and Compliance. [redacted] said that she and [redacted] are knowledgeable "of the law" and they both know that an Intelligence-Related Incident Report should have been submitted within 24 hours to SID Oversight and Compliance. [redacted] said that management "dropped the ball" by not reporting this FISA violation.

(b) (3)-P.L. 86-36

(b)(3)-P.L. 86-36
(b)(6)

(U//~~FOUO~~) said that she eventually submitted the Intelligence-Related Incident Report on behalf of the branch on 26 September 2013 after being interviewed by the OIG. said that she and discussed submitting the incident report with their management who agreed that this report should have been filed on 10 September 2013. submitted the Intelligence-Related Incident Report on 26 September because who is a part-time employee, had reached the end of her work day. and did not want to wait any longer to submit this report to SID Oversight and Compliance.

(U//~~FOUO~~) said that the FISA information in question was not accessible to analysts and that queries could not have been made against it. Agency analysts do not have access to the data storage area where this FISA information was stored. The FISA information was being stored in a area which had been created to comply with Agency continuity of operations planning.

(b)(3)-P.L. 86-36

(U//~~FOUO~~)

(U//~~FOUO~~) was interviewed on 14 January 2014 and provided the following sworn testimony.

(U//~~FOUO~~) said that on 9 September 2013 a contractor assigned to the branch discovered FISA information in a data repository that had exceeded the one-year retention authority. The FISA information had escaped detection and deletion because the age off scripts were written to capture FISA information

(U//~~FOUO~~) said that and asked him to confirm that FISA information was being retained longer than one year. He was able to confirm the violation and told and said that he immediately wrote new program scripts that identified and deleted any FISA information that was being retained longer than one year. In all, he found zip files that contained FISA information. All of this FISA information was deleted. said that analysts did not have access to this data repository and could not query this information.

(U//~~FOUO~~) said that he did not know if submitted an Intelligence-Related Incident Report. said that his responsibility is to recognize a compliance violation and report it to his branch management. He knew this violation had been reported to and because he was asked to verify the unauthorized retention. said that he was fixated on writing new age off scripts to bring the office into compliance and he did not think about who was going to report the violation.

(b)(3)-P.L. 86-36
(b)(6)

(U) ANALYSIS AND CONCLUSION

(U//~~FOUO~~) was notified of the FISA retention violation on 9 September 2013, the day the violation was discovered. directed a subordinate to find out the details of the retention violation. also prudently notified her immediate management of the violation via email. However, failed to submit an Intelligence-Related Incident Report as required. testified that she should have submitted an Intelligence-Related Incident Report once she was notified of the FISA retention violation. said that she wanted to get additional details from the analyst who was reviewing the extent of the incident but that she forgot to ask for that information. An Intelligence-Related Incident Report was eventually submitted on 26 September 2013 after was interviewed by the OIG.

(U//~~FOUO~~) The instructions for completing the Intelligence-Related Incident Report states that the form "…should be used to submit both initial and final incident reports. Please complete as much information with the initial incident report as is available at the time of submission." The report submission process allows for an initial report to be submitted with partial information and a later report with more details to be submitted. It is understandable for to want the complete details of this event but she should have fulfilled her reporting obligations by submitting a timely, initial report.

(U//~~FOUO~~) United States Signals Intelligence Directive SP0019 requires the reporting of any non-compliant activity to Oversight and Compliance upon recognition or as soon as practicable. FISA and FISA Amendments Act incidents need immediate reporting so that external overseers can be notified. The SID Oversight and Compliance FISA-Related Responsibilities Memorandum states that notice be provided as soon as possible upon recognition of any FISA incident stemming from improper retention.

(U//~~FOUO~~) All Agency employees have the responsibility to report non-compliant activity upon recognition or as soon as practicable. As the Chief of received notice of a FISA retention violation from a contractor assigned to her branch and tasked a subordinate to determine the extent of the violation. Once was notified of the incident she should have made a report, or as a manager ensured a report was made, as required by regulation recognized this obligation when she testified that she should have submitted an Intelligence-Related Incident Report but failed to do so.

(U//~~FOUO~~) Based on the above information, we conclude that failed to report a FISA incident (retention violation) upon recognition, or as soon as practicable, in violation of USSID SP0019 and SID Oversight and Compliance Memorandum, FISA-Related Responsibilities.

(b)(3)-P.L. 86-36

IV. (U) RESPONSE TO TENTATIVE CONCLUSION

(U//~~FOUO~~) The OIG's Tentative Conclusion was sent to [redacted] on 5 June 2014. [redacted] provided the following response to the OIG's Tentative Conclusion on 23 June 2014.

(U//~~FOUO~~) "I, [redacted] am aware of the mistake I've made. I've learned from it and will not allow it to happen again. While working more closely with the [redacted] compliance officer, several other incidents have been brought to my attention since this one. Each corresponding report has been entered in a timely fashion."

[redacted]
(b)(3)-P.L. 86-36

[redacted]
(b)(3)-P.L. 86-36
(b)(6)

V. (U) CONCLUSION

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that [redacted] failed to report a FISA incident (improper retention) upon recognition, or as soon as practicable, in violation of USSID SP0019, NSA/CSS Oversight and Compliance Policy, and SID Oversight and Compliance Memorandum, FISA-Related Responsibilities.

(b)(3)-P.L. 86-36

VI. (U) DISTRIBUTION OF RESULTS

(U//~~FOUO~~) This report of investigation will be provided to M/ER for information and appropriate action.

[redacted]
Senior Investigator

(b)(3)-P.L. 86-36

Concurred by:

[redacted]
Assistant Inspector General
for
Investigations

Appendix A

Applicable Authorities

(U//~~FOUO~~) United States Signals Intelligence Directive USSID SP0018, Legal Compliance and U.S. Persons Minimization Procedures, 25 January 2011

Section 5 – (U) Domestic Communications
(b) (U) Retention (2) b.

(U) In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is one year unless the Deputy Director for Operations, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements.

Section 6 – (U) Foreign Communications of or Concerning United States Persons
(a) (U) Retention (1) b.

(U) IN the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is one year unless the Deputy Director for Operations, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements.

(U//~~FOUO~~) United States Signals Intelligence Directive USSID SP0019, NSA/CSS Signals Intelligence Directorate – Oversight and Compliance Policy, 13 November 2012

Section 3 – (U) Responsibilities
(U) Individuals and Managers, 3.6

(U) Every individual must comply with applicable laws, statutes, directives, and regulations by:

(U//~~FOUO~~) Reporting any non-compliant activity to management, an IOO, SV, and OIG.

Section 4 – (U) Policy and Procedures
(U) 4.1 Five Foundational Components of Compliance:

No. 4. (U) Reporting of non-compliant activity.

(U) Reporting Incidents of Non-Compliance

(U//~~FOUO~~) All incidents of SIGINT mission non-compliance must be reported to SV and the OIG in accordance with established guidelines as follows:

(U) When and how should the incident be reported?

(U//~~FOUO~~) An incident must be reported to local management, SV, and the OIG, with a copy sent to the sponsoring mission owner, upon recognition, or as soon as practicable…Updates to the initial incident report must be filed as additional information becomes available. For FISA and FISA Amendments Act incidents, NSA/CSS is responsible to also report incidents immediately upon recognition to the NSA/CSS OGC, which may report the information to external customers.

(U//~~FOUO~~) SID Oversight and Compliance FISA-Related Responsibilities – INFORMATION MEMORANDUM, 10 August 2006

(U//~~FOUO~~) Individual Responsibilities

(U//~~FOUO~~) L. To notify SID Oversight and Compliance immediately of an FISA incidents that stem from improper collection, processing, retention, and/or dissemination. A formal write-up providing the details of the incident, routed through the appropriate signature chain, should be provided to SID Oversight and Compliance as soon as possible upon recognition of the incident.

Appendix B

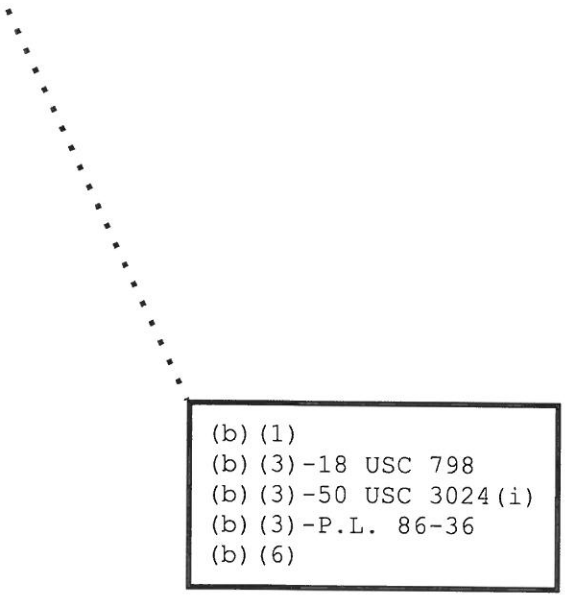
(U//~~FOUO~~) NSA/CSS Intelligence-Related Incident Report

26 Sept 2013

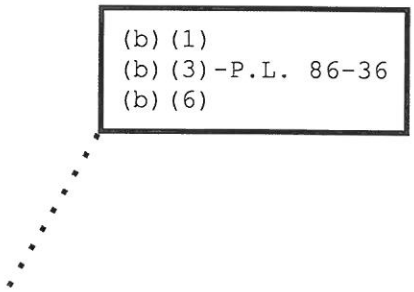
The minimum classification for this form is SECRET//COMINT//REL TO USA, FVEY. The classification may be higher based on information input into the form. See the "Overall Incident Classification" field on page 1.

(U) NSA/CSS Intelligence-Related Incident Report

(b)(1)
(b)(3)-P.L. 86-36
(b)(6)


(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)


(b)(1)
(b)(3)-P.L. 86-36
(b)(6)

Appendix C

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Email from [redacted] to [redacted] management, 26 September 2013

(b)(3)-P.L. 86-36
(b)(6)

(b)(3)-P.L. 86-36
(b)(6)

From:
Sent: Thursday, September 26, 2013 4:40 PM
To:
Cc:
Subject: (U) Expired FISA found in system
Attachments: Draft 26Sept2013_Incident_Report.pdf
Signed By:

(b)(3)-P.L. 86-36

Classification: ~~TOP SECRET//SI//NOFORN~~

and I were called by from the IG office asking us to meet with him because he had information of a potential FISA violation. We both provided formal statements that were recorded. From the discussions we had with him it was because of not reporting a FISA incident.

We want you to have the details:

After the discussion with we talked with and obtained guidance that we should formally submit the FISA incident report. I have found the form and filled in a very small portion, as is the only one with the details on the required changes to the script, the volume of data removed, and whether it was data removed. We have included a first draft of the incident report and would like to await return from TDY before having it formally submitted.

and I are both on leave Friday, 27 September 2013 but I've included in this email as she may be able to assist if actions are required tomorrow. is expected back from TDY on Monday, 30 September 2013.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Apologize for not reporting immediately.

(b) (3)-P.L. 86-36

(U//~~FOUO~~)

[redacted]

JSignout status: [redacted]

Dropbox [redacted]

From: [redacted]
Sent: Thursday, September 26, 2013 12:49 PM
To: [redacted]
Cc: [redacted]
Subject: FW: (U//~~FOUO~~) Expired FISA found in our [redacted] system

Classification: ~~TOP SECRET//SI//NOFORN~~

[redacted]

(U) Let's discuss the results of your investigation as soon as you return to the office on Monday. I will follow with proper reporting at that time.

Thanks!

[redacted]

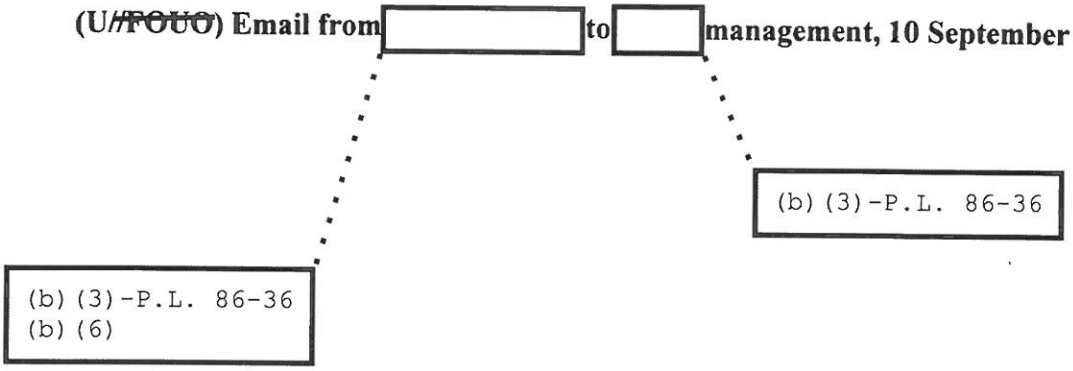
(b) (3)-P.L. 86-36
(b) (6)

JSignout status: [redacted]

Dropbox: [redacted]

Appendix D

(U//~~FOUO~~) Email from [redacted] to [redacted] management, 10 September 2013



From:
Sent: Tuesday, September 10, 2013 8:44 PM
To:
Cc:
Subject: FW: (U//~~FOUO~~) Expired FISA found in our system

(b)(3)-P.L. 86-36

Classification: ~~TOP SECRET//SI//NOFORN~~

All,

~~(TS//SI//NF)~~ Just wanted to make you aware that last night, stayed late to delete the said FISA files below. We will follow with a better summarization for you after investigates if additional FISA data exists in the filesystem that should have been aged off.

Thanks!

(b)(3)-P.L. 86-36
(b)(6)

JSignout status:
Dropbox:

From:
Sent: Monday, September 09, 2013 4:27 PM
To:
Cc:
Subject: (U//~~FOUO~~) Expired FISA found in our system

Classification: ~~TOP SECRET//COMINT//NOFORN~~

A brief summary of events :

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted] I immediately went to management and reported the discovery.

--

(U//~~FOUO~~)

[redacted]

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

DERIVED FROM: NSA/CSS 1-52
DATED: 08 January 2007
DECLASSIFY ON: ~~20320108~~

Classification: ~~TOP SECRET//COMINT//NOFORN~~

Classified By [redacted]

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: ~~20380901~~

Classification: ~~TOP SECRET//SI//NOFORN~~